



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,924	04/26/2001	Craig S. Skinner	PALM-3609.US.P	8278
49637 7590 04/20/2007 BERRY & ASSOCIATES P.C. 9255 SUNSET BOULEVARD SUITE 810 LOS ANGELES, CA 90069			EXAMINER COLIN, CARL G	
			ART UNIT 2136	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			04/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/844,924

Applicant(s)

SKINNER, CRAIG S.

Examiner

Carl Colin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 January 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-31 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-31 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/26/2007, applicant has amended claims 1, 13, and 20, the following claims 1-31 are presented for examination.

2. Applicant's remarks, pages 11-13, filed on 1/26/2007, with respect to the rejection of claims 1-31 have been fully considered, but they are not persuasive. Applicant indicated,

"The present invention, as recited in independent claims 1, 13 and 20, is directed to a method and system of securing a handheld computer against backdoor test applications to maintain the integrity of wireless networks which the handheld computer is connected to. The handheld computer is backdoor enabled so that backdoor test applications may be executed on the devices."

However, the claims do not recite any limitations about backdoor applications nor any execution of backdoor test applications. Applicant adds,

Such overhead of bits on the entitlement key is not necessary in the present invention. The present invention contemplates a single record containing only a copy of the serial number and the authorization level.

Siefert does not overcome the shortcomings of the Beetcher reference. Siefert is directed to assigning key codes for computer resources. Siefert also provides for numerous fields in the key code, where such overhead is impractical on a handheld computer with limited resources (see Fig. 4). Therefore, Siefert does not disclose or suggest "a single encrypted record" containing "only a copied serial number and a first authorization level."

As mentioned in the last Office Action, the claimed "authorization level" can be reasonably and broadly interpreted as containing plurality of fields or bits. Therefore, Beetcher discloses a single encrypted entitlement key containing only a serial number and entitlement bits that meets the recitation of single encrypted record containing only a serial number and a first authorization level as shown below.

Art Unit: 2136

Beetcher discloses an encrypted entitlement key that enables execution of the software. "The key includes the serial number of the computer for which the software is licensed, together with a plurality of entitlement bits indicating which software modules are entitled to run on the machine." (see abstract)

Also, contrarily to applicant's arguments, the claim is not directed to a handheld computer nor recites a handheld computer with limited resources. Again the claim has been reasonably and broadly interpreted for merely reciting "enabling an electronic device to run a controlled application with a single encrypted record containing only a serial number and a first authorization level." The claims have been amended to recite "wherein said electronic device is backdoor enabled" Applicant also argues that

"There is no prima facie case of obviousness since neither reference discloses an electronic device which is backdoor enabled."

Examiner respectfully disagrees because the claimed limitation as recited in (a) already defines that a device is backdoor enabled by authorizing said electronic device to run controlled applications having authorization levels not exceeding said first authorization level. The enabled application enables the electronic device as described on page 23 of the original specification.

In a preferred embodiment, Beetcher discloses authorizing the electronic device to run other software modules with the same product number and limited features (wherein the authorization level does not exceed the first authorization level) (see column 11, lines 40-56) that meets the recitation of a device that is backdoor enabled. Also there is disclosure of an unlock routine that can unlock program in response to user input (see column 9, line 50 through column 10, line 22) that also meets the recitation of a device that is backdoor enabled. Siefert also discloses a device that enables access to lower level application (see column 4, lines 45-56;

Art Unit: 2136

column 7, lines 35-40; and column 9, lines 12-24) that the recitation of a device that is backdoor enabled. Therefore, applicant has not overcome the rejection by amending the claims, and claims 1-31 remain rejected in view of the prior art.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,933,497 to **Beetcher et al.** in view of US Patent 6,526,512 to **Siefert et al.**.

As per claims 1 and 20, Beetcher et al. substantially discloses a method of security comprising the steps of: enabling a computer system to execute a software module with an encrypted entitlement key containing a serial number and entitlement bits that meets the recitation of *a) enabling an electronic device to run a controlled application with a single encrypted record containing only a copied serial number and a first authorization level, for*

Art Unit: 2136

example (see abstract); **Beetcher et al.** discloses that each customer receives an entitlement key enabling the customer to run only those software modules to which he is entitled (column 4, lines 40-45) that meets the recitation of wherein said first authorization level authorized said electronic device to run controlled applications having authorization levels not exceeding said first authorization level. **Beetcher** also discloses other entitlements such as charge group, key type, serial number of the machine, and product entitlement field assigned to the device (see column 6, lines 20-40). In another embodiment, **Beetcher et al** discloses in column 7, lines 1-16, other authorization levels that are hardware specific assigned to said electronic device. There is suggestion in column 2, lines 49-53 that other entitlement may also be machine specific entitlement or authorization level assigned to a machine to make sure that a software is authorized to run on a specific machine. **Beetcher et al** discloses authorizing the electronic device to run other software modules with the same product number and limited features (wherein the authorization level does not exceed the first authorization level) (see column 11, lines 40-56) that meets the recitation of *wherein said electronic device is backdoor enabled*. Also there is disclosure of an unlock routine that can unlock program in response to user input (see column 9, line 50 through column 10, line 22) that also meets the recitation of a device that is backdoor enabled. *b) verifying said electronic device is correctly enabled*, for example (see column 6, line 65 through column 7, line 47); and *c) verifying said first authorization level is of sufficient authority to run said controlled application on said electronic device*, for example (see column 6, line 65 through column 7, line 47); and *wherein a second authorization level of said controlled application does not exceed the first authorization level* (column 7, lines 1-65).

Beetcher et al suggests to add protection by using entitlement that contains machine specific

Art Unit: 2136

information and encoding it into the software itself. The citations with respect to version level (column 6, lines 20-40), four levels of hardware and software (column 7), limited functions of the software modules (see column 11, lines 40-56) are being interpreted as different authorization levels. To provide further support of disclosure of different access levels for access authorization, **Siefert et al.** in an analogous art teaches key codes containing authorization levels (column 2, lines 40-65) and the key codes (authorization levels) are assigned to an electronic device and authorizes said electronic device to run controlled applications having authorization levels not exceeding said first authorization level (see column 4, line 44 through column 5, line 55). **Siefert et al.** discloses how the authorization levels are compared to determine access upon launching a program request (see column 8, lines 50-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Beetcher et al** to include the step of wherein the first authorization level is assigned to the electronic device and authorizes the electronic device to run controlled applications having authorization levels not exceeding the first authorization level as taught by **Siefert et al** (see column 4, line 44 through column 5, line 55). One of ordinary skill in the art would have been motivated to do so because the teaching of **Siefert** provides detecting and controlling any program that is required to pass the security process by doing the following: when a program launch is requested, running a key code process of comparing the key code of the computer with that of the program to be run in order to authorize execution of the program upon meeting predetermined criteria. One of ordinary skill in the art would have recognized the advantage of preventing hacker from learning the identities of the key codes and preventing hacker from learning how the security process run by assigning key codes (authorization levels)

Art Unit: 2136

to both the computer and the program by a match determination process and using region of memory non-accessible to users to store the key codes (authorization levels) as suggested by **Siefert et al** (column 7, lines 15-25 and column 7, line 50 through column 8, line 35 and column 8, lines 50-67).

As per claims 2, 14, and 21, Beetcher et al. discloses the limitation of wherein step a) comprises the steps of: a1) fetching a serial number uniquely associated with said electronic device, said serial number located on said electronic device, for example (see column 7, lines 17-47); a2) copying said serial number, forming said copied serial number that is identical to said serial number, for example (see column 6, lines 20-40); a3) creating a record that contains said copied serial number and said first authorization level, said first authorization level previously assigned to said electronic device, for example (see column 6, lines 20-40); a4) encrypting said record, forming said encrypted record, for example (see column 4, lines 57-65 and column 8, lines 53-65); and a5) storing said encrypted record in said electronic device, for example (see column 8, lines 53-65). These claims are also rejected on the same rationale as the rejection of claim 1 for reciting “said first authorization level previously assigned to said electronic device”.

As per claims 3 and 22, Beetcher et al. discloses the limitation of wherein step b) comprises the steps of: b1) locating said encrypted record, for example (see column 9, line 40 through column 10, line 20); b2) decrypting said encrypted record, if said encrypted record is located, for example (see column 9, line 40 through column 10, line 20); b3) reading said copied serial number from said encrypted record, if said encrypted record is successfully decrypted (see

Art Unit: 2136

column 10, lines 27-31 and 43-47); b4) fetching said serial number, for example (see column 9, line 40 through column 10, line 20); and b5) comparing said serial number and said copied serial number, for example (see column 9, line 40 through column 10, line 20 and column 13, lines 1-8).

As per claims 4 and 23, Beetcher et al. discloses the limitation of wherein step b) comprises the further step of executing said controlled application on said electronic device, said controlled application having controlled attributes, for example (see column 6, lines 40-67);

As per claims 5, 12, 24, and 31, the combination of **Beetcher et al** and **Siefert et al** discloses the limitation of wherein said step c) comprises the steps of: c1) reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match, for example (see **Beetcher et al**, column 9, lines 40-67 and column 10, lines 20-67); c2) comparing said first authorization level with a second authorization level assigned to said controlled application (**Beetcher et al**, column 10, lines 40-47 and column 7); and c3) allowing access to said controlled attributes of said controlled application, if said first authorization level is of an equal or higher authorization level than said second authorization level, for example (see **Beetcher et al**, column 10, lines 20-47 and column 4, lines 34-46). **Siefert et al** also discloses (see column 4, lines 45-56; column 7, lines 35-40) comparing first authorization level with second authorization level to authorize the computer to run controlled applications as discussed in claim 1. Therefore, these claims are also rejected on the same rationale as the rejection of claim 1.

As per claims 6, 15, and 25, **Beetcher et al.** discloses the limitation of wherein step a) is performed with object code instructions that meet the recitation of an enabler application, said enabler application enabling said electronic device to run applications having authorization levels equal to or lower than said first authorization level, for example (see column 8, lines 48-67 and column 4, lines 34-46).

As per claims 8, 9, 18, 19, 27, and 28, the combination of **Beetcher et al** and **Siefert et al** discloses the limitation of comprising the further step of: aborting said application and denying access if any of the following conditions are met: said encrypted record is not successfully located in step b1) ; said encrypted record is not successfully decrypted in step b2); said serial number and said copied serial number do not match in step b5); or said first authorization level is of a lesser value than said second authorization level in step c2) , for example (see **Beetcher et al**, column 8, lines 48-67 and column 4, lines 34-46 and column 10, lines 20-67).

As per claims 13 and 16, **Beetcher et al.** substantially discloses a method of security and executable as a computer program comprising the steps of: *a) executing an application on an electronic device, said application having controlled attributes* (see abstract). **Beetcher et al** discloses authorizing the electronic device to run other software modules with the same product number and limited features (wherein the authorization level does not exceed the first authorization level) (see column 11, lines 40-56) that meets the recitation of *wherein said*

Art Unit: 2136

electronic device is backdoor enabled. Also there is disclosure of an unlock routine that can unlock program in response to user input (see column 9, line 50 through column 10, line 22) that also meets the recitation of wherein said electronic device is backdoor enabled. **Beetcher et al** discloses *b) locating a single encrypted record that is stored in said electronic device* (see column 8, lines 53-65), *said encrypted record containing only a copied serial number and a first authorization level, wherein said first authorization level authorizes said electronic device to run applications with controlled attributes having authorization levels not exceeding said first authorization level* for example (see abstract); **Beetcher et al.** discloses that each customer receives an entitlement key enabling the customer to run only those software modules to which he is entitled (column 4, lines 40-45) that meets the recitation of *wherein said first authorization level authorized said electronic device to run controlled applications having authorization levels not exceeding said first authorization level.* **Beetcher** also discloses other entitlements such as charge group, key type, serial number of the machine, and product entitlement field assigned to the device (see column 6, lines 20-40). In another embodiment, **Beetcher et al** discloses in column 7, lines 1-16, other authorization levels that are hardware specific assigned to said electronic device. There is suggestion in column 2, lines 49-53 that other entitlement may also be machine specific entitlement or authorization level assigned to a machine to make sure that a software is authorized to run on a specific machine. The citations with respect to version level (column 6, lines 20-40), four levels of hardware and software (column 7), limited functions of the software modules (see column 11, lines 40-56) are being interpreted as different authorization levels. **Beetcher et al** discloses *c) decrypting said encrypted record, if said encrypted record is successfully located,* for example (see column 9, line 40 through column 10,

Art Unit: 2136

line 20); d) *fetching a serial number, if said encrypted record is successfully decrypted* (see column 10, lines 27-31 and column 9, lines 50-67), *said serial number uniquely associated with said electronic device and located on said electronic device* (see column 9, lines 30-33); e) *reading said copied serial number from said encrypted record that is decrypted, if said encrypted record is successfully decrypted* (see column 10, lines 27-31 and 43-47); f) *comparing said serial number and said copied serial number, for example* (see column 9, line 40 through column 10, line 20 and column 13, lines 1-8); g) *reading said first authorization level from said encrypted record that is decrypted, if said serial number and said copied serial number match, for example* (see **Beetcher et al.**, column 9, lines 40-67 and column 10, lines 20-67); h) *comparing said first authorization level with a second authorization level assigned to said application* (see column 10, lines 40-47 and column 7), *said first authorization level previously assigned to said electronic device, for example* (see column 6, lines 20-40); i) *allowing access to said controlled attributes of said application, if said first authorization level is of an equal or higher authorization level than said second authorization level* (see column 10, lines 20-47; column 4, lines 34-46; and column 13, lines 1-8). To provide further support of disclosure of different access levels for access authorization, **Siefert et al.** in an analogous art teaches key codes containing authorization levels (column 2, lines 40-65) and the key codes (authorization levels) are assigned to an electronic device and authorizes said electronic device to run controlled applications having authorization levels not exceeding said first authorization level (see column 4, line 44 through column 5, line 55). **Siefert et al.** discloses how the authorization levels are compared to determine access upon launching a program request (see column 8, lines 50-57). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention

Art Unit: 2136

was made to modify the method of **Beetcher et al** to include the step of wherein the first authorization level is assigned to the electronic device and authorizes the electronic device to run controlled applications having authorization levels not exceeding the first authorization level as taught by **Siefert et al** (see column 4, line 44 through column 5, line 55). One of ordinary skill in the art would have been motivated to do so because the teaching of **Siefert** provides detecting and controlling any program that is required to pass the security process by doing the following: when a program launch is requested, running a key code process of comparing the key code of the computer with that of the program to be run in order to authorize execution of the program upon meeting predetermined criteria. One of ordinary skill in the art would have recognized the advantage of preventing hacker from learning the identities of the key codes and preventing hacker from learning how the security process run by assigning key codes (authorization levels) to both the computer and the program by a match determination process and using region of memory non-accessible to users to store the key codes (authorization levels) as suggested by **Siefert et al** (column 7, lines 15-25 and column 7, line 50 through column 8, line 35 and column 8, lines 50-67).

As per claim 17, Beetcher et al. discloses the limitation of wherein the same encryption/decryption protocol is used in performing steps c) and m), for example (see column 13, lines 5-18).

As per claims 7 and 26, Beetcher et al. substantially teaches the claimed method of claims 6 and 25. **Beetcher et al.** does not explicitly teach removing said enabler application

Art Unit: 2136

from said electronic device after successfully completing step a). However, **Siefert et al.** in an analogous art teaches control access to enhance security of resources where a match determination process can take actions of erasing part or all of the program to defeat running of the program, for example (see column 7, lines 35-40). **Siefert et al.** also adds, hiding process/codes or removing or placing them in separate memory or non-accessible memory locations can prevent hackers to trace the logic of codes, for example (see column 7, line 40 through column 8, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Beetcher et al.** to remove said enabler application from said electronic device after successfully completing step a) as taught by **Siefert et al.** One skilled in the art would have been lead to make such a modification because it would make the security process non accessible to hackers, as suggested by **Siefert et al** for example (see column 7, line 40 through column 8, line 35).

As per claims 10-11 and 29-30, **Beetcher et al.** discloses locking in memory the version number the product number, serial number etc. and also discloses codes stored in read-only memory (ROM) to make it not capable of alteration by customers, for example (see column 7, lines 15-30 and column 9, lines 49-67). It is well known in the art of computer security that computers have flash memory and using a flash memory will not depart from the spirit and scope of the invention of **Beetcher et al.**. **Siefert et al.** also discloses using read-only memory (ROM) for the encrypted data and serial number. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to store said encrypted record and serial number in locked flash record in said electronic device as suggested by **Beetcher et al.**

Art Unit: 2136

One skilled in the art would have been lead to make such a modification to prevent alteration of these data by customers.

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

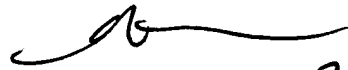
cc

Carl Colin

Patent Examiner

April 11, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


4/13/07